



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/090,422

02/28/2002

Lauri Paatero

944-005.2

6221

4955

7590

07/07/2006

WARE FRESSOLA VAN DER SLUYS &  
ADOLPHSON, LLP  
BRADFORD GREEN, BUILDING 5  
755 MAIN STREET, P O BOX 224  
MONROE, CT 06468

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 07/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/090,422	<b>Applicant(s)</b> PAATERO, LAURI	
	<b>Examiner</b> Eleni A. Shiferaw	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 April 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-65 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-65 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/25/2006 has been entered.

### *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-65 are rejected under 35 U.S.C. 102(b) as being anticipated by Hayashi Seiichiro JP 09-261218

Regarding claims 1, 29, and 58, Seiichiro teaches a method/system comprising:

having an identity authenticated in a first system (0005; *computer 2 with authenticated certification*);

a second system causing a key to be generated for use in the second system  
(Abstract 5-6 and 0006; *computer 2 generates a public key A for the computer 2 and/or verification center 1*);

Art Unit: 2136

the second system generating a certificate for the key (0005, and 0010; *computer 2 generating certificate for the public key A*); and

establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system (Abstract, and 0010-0011; *computer 2 generating digital signature for the public key A using the authenticated identity of computer 2*).

Regarding claims 30, 59, 60, and 65, Seiichiro teaches a system/apparatus/method for authenticating a user of a second system where the user has an authenticated identity in a first system, wherein the device forms part of the second system comprising:

means for generating a key for use in the second system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2 and/or verification center 1*);

means for generating a certificate for the key (0005, and 0010; *computer 2 generating certificate for the public key A*);

means for transferring the certificate to a device forming part of the first system (Abstract solution lines 5-8), said device of the first system having information concerning the authenticated identity of the user in the first system (0005; *computer 2 with authenticated certification*), so as to establish the identity of the user in the second system by signing the certificate using the authenticated identity of the user in the first system (Abstract, and 0010-0011; *computer 2 and/or verification generating digital signature for the public key A using the authenticated identity of computer 2*); and

Art Unit: 2136

wherein said device of the second system further comprises means for receipt of said signed certificate (Abstract solution lines 6-14; *verification center 1 signs the key and returns it to computer 2*) and means for transferring the signed certificate to a third party of said second system (Abstract lines 8-22, and 0011; the resulting information is sent to computer 3).

Regarding claims 2, 31, 32, 61, and 62, Seiichiro teaches a method/system/apparatus, wherein the key is generated by the second system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2*).

Regarding claim 3, Seiichiro teaches a method, wherein the key is generated by the first system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2*).

Regarding claims 4 and 33, Seiichiro teaches a method/system, further comprising the step of: a third party communicating with the user of the second system and verifying the user of the second system by the authenticated identity of the user of the first system (0012 and 0013 lines 6-7; *computer 3 and verification*).

Regarding claims 5 and 34, Seiichiro teaches a method/system, wherein the third party is a server (0015-0016).

Regarding claims 6 and 35, Seiichiro teaches a method/system, wherein the key comprises a private-public key pair and where the certificate includes the public key of

Art Unit: 2136

the key pair (0013).

Regarding claims 7 and 36, Seiichiro teaches a method/system, wherein the certificate further includes an identity which is the same as the authenticated identity of the user of the first system (0005).

Regarding claims 8, 11, 14, 27, 37, 40, 43, 56 and 63, Seiichiro teaches a method/system/apparatus, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a Certification Authority (0013), and where the signing of the second system generated certificate is by hashing at least some data in the certificate to obtain a hash value (0014-0015), encrypting this hash value using the private key of the first system private-public key pair, and adding the encrypted hash value to the certificate (0011 lines 7-9).

Regarding claims 9, 12, 18, 22, 38, 41, 47, and 51, Seiichiro teaches a method/system/apparatus, wherein the private key of the first system private-public key pair is stored in a wireless identity module forming part of the second device (Examiner takes an official notice on storing/performing Seiichiro's method of making a second device a part of a first device in wireless devices system or storing the private key of the first system private-public key pair in a wireless identity module because the second wireless device would be a part of the communication and identified/authenticated).

Art Unit: 2136

Regarding claims 10, 13, 15-15, 39, 42, 44-45, and 64, Seiichiro teaches a method/system/apparatus, wherein prior to signing the certificate for the key for use in the second system, the user of the first system obtains access to its private key by entry of a password (PIN) (The examiner takes an official notice on the first system requiring a password authentication prior/PIN to signing certificate because it would enhance security see, Bradley et al. Pub. No.: US 2002/0194219 A1 par. 0256-0263).

Regarding claims 17 and 46, Seiichiro teaches a method/system, wherein the certificate for the key includes the full certification tree for the key, said full certification tree including a certificate of the first system for the user of the first system (0005).

Regarding claims 19 and 48, Seiichiro teaches a method/system, wherein the second system a computer connected to the Internet (0007).

Regarding claims 20 and 49, Seiichiro teaches a method/system, wherein the second system uses a security protocol for establishing a secure session (0004-0009).

Regarding claims 21 and 50, Seiichiro teaches a method/system, wherein the security protocol is selected from the group consisting of Transport Layer Security, IP Security Protocol and Secure Socket Layer (0009-00011).

Regarding claims 23 and 52, Seiichiro teaches a method/system, wherein the WIM

Art Unit: 2136

contains a private key of the user of the first system and wherein a corresponding public key of the user of the first system is certified by a Certification Authority (0005).

Regarding claims 26 and 55, Seiichiro teaches a method/system, wherein an accepted operation is the use of the key for use in the second system for encryption of data but not for signature verification (0013-0016).

Regarding claims 28 and 57, Seiichiro teaches a method/system, where the first and second users are the same entity (0005).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 24-25 and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hayashi Seiichiro JP 09-261218 in further view of Hurtado et al. (Hurtado, Patent No.: US 6,418,421 B1).

Regarding claims 24 and 53, Seiichiro fails to disclose usage limitations. However Hurtado discloses a method/system, wherein the certificate for the key for use in the second system contains one or more usage limitations (Hurtado col. 9 lines 56-65, and fig. 5 element 533).



Art Unit: 2136

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Hurtado within the system of Seiichiro because they are analogous in certificate and digital signature (Hurtado col. 24 lines 58-63). One in the art would have been motivated to incorporate the teachings of Hurtado into Seiichiro because it would specify content usage conditions by granting or restricting access to the user (Hurtado col. 12 lines 25-27).

As per claims 25 and 54, Seiichiro teach all the subject matter as described above. In addition, Hurtado teaches a method/system, wherein one usage limitation is that a third party of the second system should accept the key for use in the second system only for certain types of operations (Hurtado col. 9 lines 56-65, and fig. 5 element 533). The rational for combining are the same as claim 24 above.

### ***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E. S.  
*Eli Shif*  
6/29/06

*Ayaz Sheikh*  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100